Office of Personnel Management (OPM) Data Breach

A briefing for use by DON commanders and supervisory staff

http://www.secnav.navy.mil/OPMBreachDON

Incident Background

- **Cyber Incident 1, announced June 4, 2015**
  - ~4.2 M current and former **civilian** employees impacted by a cybersecurity incident (December 2014)
  - Personal information includes: name, SSN, place and DOB, current and former addresses, education, training, employment information, etc.
  - Notification email and letters in process (begun June 8)
  - Very likely that not all personnel have been contacted

- **Cyber Incident 2, announced June 18 & July 9, 2015**
  - 19.7 million former and current employees (**military**, **civilian** and **contractor**)
  - 1.8 million others affected (spouses or co-habitants of employees)
  - 1.1 million fingerprint records
  - Detailed personal information was lost in this breach – check the SF form you submitted!
  - Notification efforts are still in planning, but will likely include notifications by both email and the U.S. Postal Service

- **eQIP – (Electronic Questionnaires for Investigations Processing) Event, suspended June 29 – July 23, 2015**
  - eQIP is used by civilian employees, service members, and contractor employees, and Human Resource and Security Managers to send standard forms 85, 85P and 86 information to OPM
  - Temporary suspension (June 26 – July 23) as precautionary measure to close identified security vulnerabilities

Incident #1
(former & current federal employees)

- **April 2015 – OPM aware of cyber incident to have occurred December 2014**
- **PII information compromised**
- **Affected civilian employees automatically covered by 18 months of free identity theft insurance up to $1 million**
  - Affected civilian employees also offered 18 months of credit monitoring **if** employees register their information with CSID
  - Credit monitoring is voluntary and you must enroll
- **Initial notification - email from OPMcio@csid.com Subsequent notification -- U.S. Postal Mail**
- **CSID – industry leader for identity theft protection**

If emails were deleted or you were not notified about Incident #1, contact CSID Toll Free at 1-844-777-2743

Incident #2 (military, civilian, contractor former & current employees)

- **Affected 21.5 million background investigation applicants, spouses or co-habitants, others**
- **Background investigation (SF85, 85p, 86) information accessed includes:**
  - SSNs
  - Residency & educational history
  - Employment history
  - Information about immediate family, personal & business acquaintances
  - Health (including mental health), criminal & financial history
  - Usernames and passwords used to fill out background investigation forms
- **Personal information of spouse or cohabitant (including SSNs) compromised**
- **If you wish to request a copy of your personnel security investigation go to:**
  https://www.opm.gov/investigations/freedom-of-information-and-privacy-act-requests/
- **Notifications have not begun and affected personnel will be notified by**

Highly likely to impact those who underwent a background investigation through OPM during 2000 or after; submissions prior to 2000 less likely

Incident #2 – Monitoring & Protection Services

- **Monitoring service provider not yet determined**
- **Identity theft insurance and other protection for at least 3 years – no charge**
- **Suite of services should include:**
  - Full service identity restoration support and victim recovery assistance
  - Identity theft insurance
  - Identity monitoring for minor children
  - Continuous credit monitoring
  - Fraud monitoring services beyond credit files

Services will be provided to impacted current/former civilian, military and contractor employees, their spouses (co-habitants) whose SSNs were compromised, and minor children

eQIP Actions

- **eQIP temporarily suspended by OPM 26 June**
  - Precautionary measure - not a result of activity on the network/no evidence of exploitation
  - eQIP is the automated system for submission of SF85, 85p and 86 to OPM for workforce suitability and clearance eligibility determinations and investigations
  - Impacts civilians, contractors, military
  - Interim solution for secret clearances/CAC card continues until further notice
- **eQIP returned to service 23 July**
  - New procedures in place for eQIP users – OPM will contact users detailing new instructions
- **USAJOBS is not impacted**

DON interim solution for secret clearances
Top secret investigations/re-investigations resume

What is DON doing?

- **Senior Level DON data breach coordination cell**
- **Committed to supporting all DON employees (civilian, military, contractor), sharing information**
  - Designated website - **http://www.secnav.navy.mil/OPMBreachDON**
  - ALNAVs – #052/15; #056/15
  - DONhrFAQs
- **Identification, development, execution of risk mitigation strategies for DON processes**

Table of Resources for Affected Individuals

Resource	Contact Info	Provides
CSID® Credit Monitoring Service	www.csid.com/opm/ U.S. toll free: 844-777-2743 International call collect: 512-327-0700	Assistance with signing up for CSID credit monitoring services for affected individuals.
Department of Navy FAQ E-mail	DONhrFAQ@navy.mil	Answers to data breach related questions.
Department of the Navy Civilian Employee Assistance Program (DONCEAP)	www.DONCEAP.foh.hhs.gov Toll free: 1-844-DONCEAP (1-844-366- 2327) TTY: 1-888-262-7848 International: 001-866-829-0270	Support for financial issues and identity theft for all DON civilians and their families.
Federal Trade Commission (FTC) Complaint Submission	www.ftccomplaintassistant.gov Toll free: 1-877-ID-THEFT (438-4338)	A clearinghouse for complaints by victims of identity theft.
Federal Trade Commission (FTC) Identity Theft Recovery Plan	Downloadable PDF: www.identitytheft.gov	A step by step guide on what to do if your identity information has been stolen.
Free Credit Report Review	www.AnnualCreditReport.com Call: 1-877-322-8228	One free credit report per year from each of the three major crediting bureaus (contact information for credit bureaus can be found on the Federal Trade Commission website: www.ftc.gov).
Guide to Keeping Your Social Media Accounts Secure	www.doncio.navy.mil/ContentView.aspx?id=5950	Safety guidelines and tips to keeping your personal information safe while using social media.
Internal Revenue Service (IRS)	http://www.irs.gov/Help-&-Resources Toll free: 1-800- 908-4490	Guidance on what to do if you suspect the improper use of identification information in connection with tax violations.
Phishing Reports	NMCS_SPAM@navy.mil	Resource to report phishing attempts.
Social Security Administration	www.socialsecurity.gov/kc/id_resources.htm Toll free: 1-800-269-0271	Guidance on what to do if you suspect your Social Security number is being fraudulently used.
TransUnion® Fraud Alert	www.transunion.com/fraud Call: 1-800-680-7289	Placing fraud alert on your credit file to let creditors know to contact you before opening a new account in your name.

Recap

What we know

- Incident #1 - Process for Identity Theft and Option for Credit Monitoring; 18 months coverage
- Incident #2 - Breadth of breach and identity theft/credit monitoring services; 3 years coverage
- eQIP (used for clearances) has returned to service
- Commands should **continue** to hire

What we don't know

- Monitoring service provider for Incident #2

What affected employees can do

- Be vigilant concerning your personal information
- Use the tools available (CSID, fraud alerts, etc.)
- Monitor SECNAV website (www.SECNAV.navy.mil/OPMbreachDON/) and FAQs
- Check out the *new* Defense Security Service Toolkit (http://pyi-toolkit.cdse.edu)
- Beware of attempts to solicit personal and work related information.
  If you are approached contact your commander, security manager and NCIS.

Questions

(Civilian, Military, Contractor)

DONhrFAQ@navy.mil

www.secnav.navy.mil/OPMBreachDON

Backup

Leadership Talking Points

- We understand the seriousness and impact that these incidents are having on our workforce, and we remain committed to keeping you updated.
- There are two cybersecurity incidents
  - Incident #1 identified in April 2015 impacted former and current federal employees and compromised personal information.
  - OPM continues to notify personnel who may be affected - it is important to emphasize that the notification is ongoing and employees should not assume they have not been impacted if they have not received notification yet
- Incident #1 — Notifications are ongoing
  - Because of the .com (dot-com) email address, some notification messages went to the junk mail folder and were deleted.
  - Employees can contact CSID to authenticate their status, receive their PIN# and register.
  - Toll free number is 1-844-777-2743 – wait times are averaging 5-6 minutes
- Incident #1 — Monitoring services
  - Complimentary identity theft insurance for 18 months. Every affected individual, regardless of whether or not they explicitly take action to enroll with their PIN#, will have up to $1 million of identity theft insurance and access to full-service identity restoration provided by CSID until December 7, 2016.
  - Enrolling in the CSID credit monitoring is voluntary on the part of civilian employees.

Leadership Talking Points (2)

- The second cyber incident was detected during the investigation of the first incident. OPM worked with DHS and FBI to determine who was affected by the second intrusion.
- Information compromised in Incident #2 included sensitive and personal information provided in background investigations.
- Incident #2 — Individuals affected will be notified by U.S. Postal Mail & email
  - Deployed military and civilians may also receive email notification if unable to contact by U.S. Postal Mail
- Incident #2 — Impacted employees include former and current military, civilian and contractor personnel, their spouses or co-habitants
- Incident #2 — Impacted employees/individuals and their minor children will receive at least 3 years of comprehensive monitoring and protection services; provider to be determined
- The Department of the Navy recognizes the impact of the OPM breach on its employees, and is committed to sharing updated information with its employees. The Department regularly updates a set of Frequently Asked Questions with the latest information
- We continue to accept questions at DONhrFAQ@navy.mil to best support our civilian workforce

Refer to DON OPM Data Breach FAQs
FAQs also available at OPM.gov

Information about OPM

- **The Office of Personnel Management** (**OPM**) is an independent agency of the United States government that provides oversight and policies governing the civil service of the federal government.
  - OPM is part of the Executive Office of the President
  - OPM provides guidance, rules, regulations and oversight for employment of most federal civilian employees of the federal government, including most DOD employees.
  - For more information go to https://www.opm.gov/

- **OPM centrally stores personal and employment related information for most federal civil service employees, to include electronic Employee Personnel Folders (eOPF)**
  - Federal agencies and employees, including DOD civilian employees, have access to an electronic folder instead of a paper record. Allows agencies and employees access from any location at any time.
  - Complies with federally mandated employee record management regulations.
  - For more information go to https://www.opm.gov/FAQs/ and search for eOPF.

- **OPM is the Personnel Suitability and Security Investigations service provider for most of the federal government, including most DOD military members, civilian employees, and contractor personnel**
  - OPM conducts suitability and security investigations based on information contained in each individual member's Standard Form 85, 85P and 86 – and results of checks of authoritative records and investigations.
  - OPM stores personal information related to these forms as well as some fingerprint information.
  - OPM also maintains investigation information developed during suitability and security investigations.
  - Once an investigation is completed, information from the standard forms and results of the investigations are forwarded to the DOD Central Adjudication Facility (DODCAF) for determination of suitability for employment and eligibility to maintain a security clearance.
  - For more information go to https://www.opm.gov/investigations/

Incident #2 – Background Information Compromised

- Social Security Numbers
- Residency and educational history
- Employment history
- Personal and business acquaintances
- Marital status
- Information about children, immediate family and other relatives
- Financial history [there is no evidence that separate systems that store information regarding the health, financial, payroll and retirement records of federal employees were impacted by the second incident (i.e., annuity rolls,
- Selective service record
- Military history
- Foreign contacts
- Foreign activities, foreign business, professional activities, foreign government contacts
- Foreign travel, passport information
- Psychological and emotional health information
- Police record, illegal use of drugs and drug activity, alcohol use
- Investigations and clearance record
- Criminal and non-criminal court cases

Some records also include findings from interviews conducted by background investigators and fingerprint investigations. Usernames and passwords that applicants used to fill out their background investigation forms were also compromised.